

Algo 8300

Provisioning Server and Device Management Guide

Need Help?

(604) 454-3792 or support@algosolutions.com



Table of Contents

INTRODUCTION 3

ADDING DEVICES TO THE DASHBOARD 4

CONFIGURE RESTFUL API 4

CONFIGURE PROVISIONING 5

DEVICE ACTIONS OPTIONS 6



Introduction

This guide aims to describe the steps required to configure the 8300 Controller as a HTTP or HTTPS provisioning server. Besides being capable of monitoring and supervising hundreds of Algo IP Endpoints (see the [user guide](#) for more details), the 8300 may be used as a provisioning server for mass deployments and firmware upgrades. Furthermore, it is possible to send API requests to one or multiple monitored devices, to perform different actions.

Adding Devices to the Dashboard

The Dashboard is where users can check the status of monitored endpoints, as well as send Device Actions to update settings, reboot monitored devices, etc.

- Browse to the 8300 web interface, log in, navigate to Dashboard -> Locator tab.
- Add the Algo endpoints to be monitored by navigating to the Locator subtab.
- The locator will find all Algo IP endpoints in the network. Alternatively, add them manually.

* Note 1: The locator is not able to find endpoints in different subnets or VLANs, even if routing is in place. These must be added manually.

* Note 2: The following Algo first generation IP endpoints may not be visible through the 8300 locator: 8180 SIP Audio Alerter (G1), 8128 SIP Strobe Light (G1), 8028 SIP Doorphone (G1), 8061 IP Relay Controller. These may be added manually.

Configure RESTful API

Enable RESTful API for the 8300 to send API commands to the monitored devices.

- In Basic Settings -> Features tab
- Set the Remote Device Admin Password and RESTful API password (default is *algo*).
- Save the changes.

The screenshot shows the web interface with the following structure:

- Navigation tabs: Status, Dashboard, **Basic Settings**, Advanced Settings, System, Logout
- Sub-tabs under Basic Settings: **Features**, Audio Alerts, Email Alerts
- Section: **Features**
- Section: **Credentials for Accessing Managed Devices**
- Text: The passwords used to manage and control remote devices in the Managed Devices list
- Field: Remote Device Admin Password (password masked with dots) with a tooltip: "Required for admin web access to remote devices during initial configuration. Including actions such as, enabling/disabling SNMP, enabling RESTful API support, and/or Rebooting devices."
- Field: Remote Device RESTful API Password (password masked with dots)

Change tabs to Dashboard-> Devices, and use the Device Actions dropdown box to:

- Enable SNMP (not required but recommended)
- Enable REST

*Note: Wait for remote device(s) to reboot after each of the above steps. The reboot process takes about 60 seconds.

Configure Provisioning

All Algo IP devices support provisioning, which is detailed on the [Algo Provisioning](#) webpage. The 8300 can act as a HTTP or HTTPS provisioning server, to host firmware files, configuration files, tone files (WAV or MP3), and certificates for mutual authentication. This is a simple and effective method to configure multiple endpoints.

Login to the 8300 web interface and navigate to Basic Settings -> Features tab.

1. Enable Provisioning by selecting **HTTP** or **HTTPS** mode
2. Set the provisioning server **Username** and **Password**

Optional: Partial Provisioning may be configured, see the [Algo Provisioning Guide](#) for details.

*Note: 1GB of storage is available on the 8300. Firmware files may be as large as 100MB. Make sure to manage available storage and delete old files as required.

The screenshot shows the 'Features' configuration page in the Algo 8300 web interface. The navigation tabs at the top include Status, Dashboard, Basic Settings (selected), Advanced Settings, System, and Logout. Under 'Basic Settings', there are sub-tabs for Features, Audio Alerts, and Email Alerts. The 'Features' section is expanded, showing three main configuration areas:

- Credentials for Accessing Managed Devices:** This section contains two password fields: 'Remote Device Admin Password' and 'Remote Device RESTful API Password'. Both fields are currently masked with dots. A help icon and text explain that the Admin Password is required for initial configuration actions like enabling/disabling SNMP or RESTful API support.
- Provisioning Server Settings:** This section allows the 8300 to act as a provisioning server. It includes:
 - 'Enable Provisioning Server': Radio buttons for Disabled, HTTP, and HTTPS (selected).
 - 'Auth User Name': A text field containing 'algo'.
 - 'Auth Password': A masked password field.
 - 'Partial Provisioning': Radio buttons for Enabled and Disabled (selected). A help icon and text explain that this option enables support for incremental provisioning files on remote devices for enhanced security.
- Monitor Settings:** This section includes a 'Monitor Interval' dropdown menu currently set to '30 seconds'. A help icon and text explain that a shorter interval leads to faster detection of offline devices but increases network traffic.

A green 'Save' button with a checkmark is located at the bottom right of the configuration area.

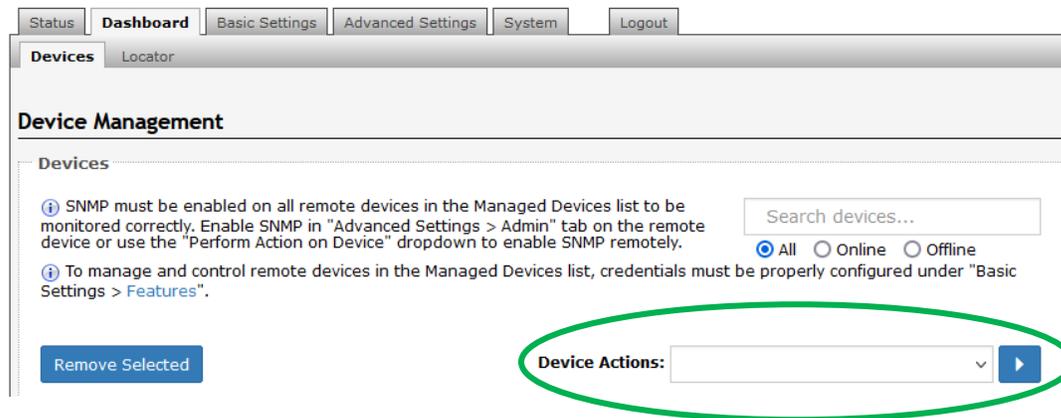
3. Navigate to Dashboard-> Devices use Device Actions to **Enable Provisioning**

To add or delete files (e.g., configuration, firmware files) go to System -> File Manager -> "prov" folder (this folder is only visible if provisioning is enabled). All file names must be formatted as described in the [Algo Provisioning Guide](#).

Once the configuration file has been added to the "prov" folder, the endpoint can be rebooted. If the steps above have been completed the endpoint will load the configuration file from the 8300. To confirm this, navigate to the Status page of the endpoint and check the "Provisioning Status". This should be listed as *Successful*. If it shows as *None Found* then please check that all previous steps have been completed or contact Algo Support.

Device Actions Options

From the main dashboard (Dashboard -> Devices tab), there are several **Device Actions** that can be selected and pushed to one or multiple device(s). See below.



- Reboot Selected
- Enable REST on Selected
- Enable SNMP on Selected
- Push Single Config to Selected
- Disable SNMP on Selected
- Enable Provisioning
- Enable REST on Selected
- Back up Config
- Update Group on Selected